

2

EUROPEAN PATENT APPLICATION

21 Application number: 90300442.2

51 Int. Cl.⁵: G07F 7/10, G07F 7/08

22 Date of filing: 16.01.90

30 Priority: 17.01.89 CA 588388

43 Date of publication of application:
25.07.90 Bulletin 90/30

84 Designated Contracting States:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

71 Applicant: Graves, Marcel Albert
14008-80 Avenue
Edmonton Alberta T4R 3J7(US)

72 Inventor: Graves, Marcel Albert
14008-80 Avenue
Edmonton Alberta T4R 3J7(US)

74 Representative: Howick, Nicholas Keith et al
CARPMAELS & RANSFORD 43 Bloomsbury
Square
London WC1A 2RA(GB)

54 **Secure data interchange system.**

57 Systems for interchanging information, for example, obtaining cash from a terminal by use of a portable device such as a credit card are well-known but suffer from being vulnerable to fraud. In the invention a highly secure information interchange system is achieved by utilizing an intelligent card (4) as the portable device which verifies that the terminal (3) is a valid one and the terminal in turn verifies that the card is valid. Unauthorized users are screened out by means of a physical characteristic scan of the user such as a finger print which is then compared with comparable data stored on the portable device (4). If an invalid terminal (3) attempts to communicate with the card (4), the card (4) erases the data and program from its memory.

EP 0 379 333 A1
 All programs and data in the terminal (3) are stored in memory which loses its contents when power is interrupted, thus improving the security of the system by making unauthorized use of a terminal very difficult. The terminal can only be brought back up by authorized personnel with their own access portable devices. Both a system and a method are claimed.

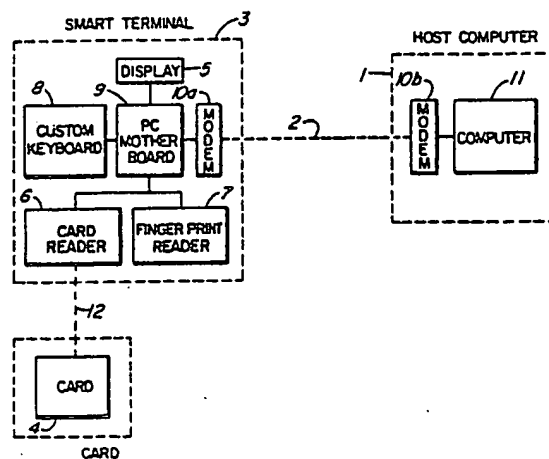


FIG. 3

2

EUROPEAN PATENT APPLICATION

21 Application number: 90300442.2

51 Int. Cl.⁵: G07F 7/10, G07F 7/08

22 Date of filing: 16.01.90

30 Priority: 17.01.89 CA 588388

43 Date of publication of application:
25.07.90 Bulletin 90/30

84 Designated Contracting States:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

71 Applicant: Graves, Marcel Albert
14008-80 Avenue
Edmonton Alberta T4R 3J7(US)

72 Inventor: Graves, Marcel Albert
14008-80 Avenue
Edmonton Alberta T4R 3J7(US)

74 Representative: Howick, Nicholas Keith et al
CARPMAELS & RANSFORD 43 Bloomsbury
Square
London WC1A 2RA(GB)

54 Secure data interchange system.

57 Systems for interchanging information, for example, obtaining cash from a terminal by use of a portable device such as a credit card are well-known but suffer from being vulnerable to fraud. In the invention a highly secure information interchange system is achieved by utilizing an intelligent card (4) as the portable device which verifies that the terminal (3) is a valid one and the terminal in turn verifies that the card is valid. Unauthorized users are screened out by means of a physical characteristic scan of the user such as a finger print which is then compared with comparable data stored on the portable device (4). If an invalid terminal (3) attempts to communicate with the card (4), the card (4) erases the data and program from its memory.

EP 0 379 333 A1
 All programs and data in the terminal (3) are stored in memory which loses its contents when power is interrupted, thus improving the security of the system by making unauthorized use of a terminal very difficult. The terminal can only be brought back up by authorized personnel with their own access portable devices. Both a system and a method are claimed.

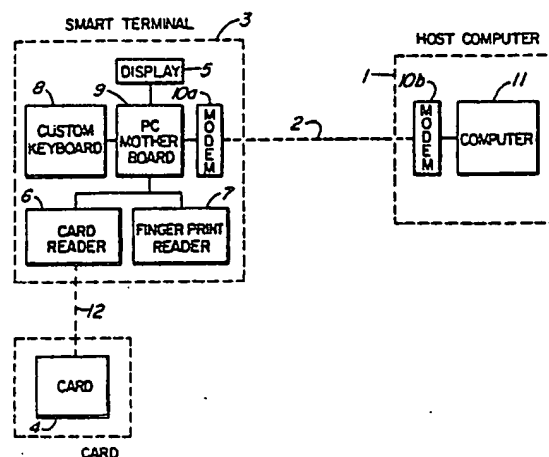


FIG. 3

SECURE DATA INTERCHANGE SYSTEM

FIELD OF THE INVENTION

This invention relates generally to a system and method of providing information and services to a population of persons through portable devices which can be used to access any of a number of terminals to make use of the services offered at the said terminals. The system and method in particular provide for security against unauthorized access. The invention has use in the fields of automatic banking, automatic credit and debit transactions, passport and travel visa verification, health and medical records, security access, licensing and any other like field where fraud may pose a problem.

BACKGROUND OF THE INVENTION

Data transfer systems using portable devices such as cards with some memory capability, for example, a magnetic strip, and terminals to which the portable devices can be connected are well known. Generally they are used to control access to some area or service. Usually the terminals are connected to a central processing unit or computer which controls access and is the ultimate storage facility for the information on the card.

British Patent 1504196 to Moreno describes such a prior art system comprised of a portable device and a peripheral device or terminal which is connected to a central computer. Many of the portable devices referred to as prior art in Moreno used magnetic track memories which could easily be modified or the contents read. Also the memory storage capacity was quite low and the memory was susceptible of accidental modification. This left such systems vulnerable to abuse from fraudulent intervention.

United States Patent 3702464 addressed the problem of lack of memory capacity and volatility by disclosing a portable device containing an integrated circuit memory. The device still suffered from the problem that the memory could be read and the contents extracted or changed. Moreno advanced the art by adding inhibiting means to prevent the transfer of data out of or into prohibited areas of the memory of the portable device. Preferably the portable device contained its own inhibiting means but the inhibiting means could be contained in the peripheral device.

In British Patent 1505715 to Moreno there is disclosed a system for interchanging information which is like those described above, but without the

error prone direct connections from the peripheral devices connected to the central computer. The peripheral devices contained a write mechanism which could transfer the information from the portable device to the peripheral device which could in turn write the information on a second portable device. These second portable devices would then be collected on some regular basis and taken to the central computer where the information would be transferred to the central computer's memory.

Canadian Patent 1207460 to Ugon discloses a method and apparatus for authorizing access to a service offered by an authorizing entity. The system comprises a portable card with memory and a microprocessor, and an authorizing entity system capable of communicating with the card and also performing computer program operations. The card and the system have the same algorithm to be executed and each has secret data upon which the algorithms operate to produce a result which can be compared to ensure that proper access is granted. This system is rather complicated and involves an operator at the authorizing entity end.

It is also known to encode a fingerprint on a portable card to verify the identity of the user. UK Patent Application GB 2185937 A of O'Shea et al discloses a credit or similar card which incorporates a computer generated image of the fingerprint of the authorized user. When a transaction is to be verified the user's finger print is scanned by a finger print reader and the result is compared with the information on the card. The user is authorized to have access if the prints match. Such devices are presently commercially available.

The systems described above suffer from the problem of complexity or they are susceptible to fraudulent and unauthorized access and tampering with the information in the card or the terminal. The present invention provides an apparatus and method for providing a highly secure and highly fraud-proof system for providing access to services of an authorizing entity.

SUMMARY OF THE INVENTION

The invention provides an improvement over previous systems and methods of authorizing access to services in a card-terminal environment by providing for a system of protection and authorization which makes the system highly fraud-proof. The system is comprised of a portable device such as a card, a peripheral device such as a terminal, and optionally, a remote host computer in the case of large systems, although it can be seen that th

host computer is not necessary for an operational system. These components are connected via some communication medium such as electrical connectors or optics or radio transmission. The terminal contains a microprocessor or some such logic device and memory, a card reading device and a finger print scanner. The card contains a microprocessor or some such logic device and memory, which can be connected to the terminal via electronic or some other means such as optics or radio transmission. The card and terminal each have their own data and programs. Upon insertion of the card into the reader a process of verification is carried out by means of the microprocessors or logic units, the programs and data in the memories. The card verifies that the terminal is valid, the terminal verifies that the card is valid and the user is verified by means of a finger print scan and comparison with finger print data previously recorded in the card. This is not to say that some other form of physical characteristic could not be used such as retinal or DNA scan. Where data is being transmitted between components of the system encoding and decoding is used to further enhance the security of the system.

The invention comprises a system for the interchange of information comprising at least one portable electronic device; at least one terminal device; communication means connecting the portable device with the terminal device; the portable device containing verification means to verify that the terminal device is a valid one; the terminal device containing verification means to verify that the portable device is a valid one and further verification means to verify that the user is authorized to use the system; protection means to prevent tampering with a terminal and encryption means to encode and decode data at the interfaces between the portable device and the terminal device.

The invention also consists of a method of preventing unauthorized access to a system comprised of a plurality of portable devices, a plurality of terminal devices and a communication link connecting the said terminal devices to a central host computer wherein the said portable device contains information identifying the said portable device as well as the authorized user, when the said terminal is connected to the said portable device and power is supplied to the said portable device the terminal device queries the portable device to determine if it is a valid portable device, if not the portable device is retained or rejected by the terminal, in turn the portable device queries the terminal to determine if the terminal is a valid terminal, if not the portable device erases its memory and becomes harmless, the terminal in turn scans a physical characteristic of the user and compares that information with

stored information on the portable device to determine if that user is authorized to use the portable device and the terminal, if the portable device and terminal are valid and the user is authorized access is allowed to the service, if not the card is retained or rejected; when the power to the terminal is interrupted the terminal programs and data are lost and can only be reloaded by authorized personnel with their access portable devices or from the host computer; encryption is used at the portable device and terminal interface as well as at the terminal and host computer interface.

BRIEF DESCRIPTION OF THE DRAWINGS

In drawings which illustrate embodiments of the inventions,

Figure 1 is a pictorial representation of the basic system components, including an optional host computer

Figure 2 is a flow chart depicting the dialog between the card and the terminal,

Figure 3 is a block diagram illustrating hardware configuration.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The combining of the capability of an intelligent card co-operating with an intelligent terminal, a finger print scanning device, and optionally interfacing with a host computer to ensure maximum possible protection for a card user and a card issuer, is very desirable. In Figure 1 the basic hardware configuration needed to implement such an idea is set out in pictorial form. The host computer system 1 can be a personal computer, mini-computer, mainframe or any suitable computer configuration depending upon the particular application. The host computer system is connected to terminal 3 by suitable linkages such as a telephone line through a modem. It is also possible to utilize other linkages such as radio transmission, or direct cable or optics. Terminal 3 is described as an intelligent terminal and comprises an output device such as a display 5, or a voice synthesizer or other means of communication with the user, a card reader 6 for reading or writing information from or to the card 4. It also contains an input device 8 such as a keyboard or other means of inputting information to the terminal and a finger print scanning device 7 or some other device to obtain physical information about the user.

When a user wishes to utilize a card to gain access to a service from a terminal, the system requires a unique verification procedure to be im-

plemented. Upon insertion of the card into the terminal, the terminal itself is verified by the card. The card is then verified by the terminal and then the user's finger print which has been digitized into the card at the time of issue is compared with the finger print which is submitted via the finger print scanning device at the time of use. Additional user identification such as a personal identification number can also be included.

If the terminal into which the card is inserted is not a valid terminal the card will erase its memory rendering itself useless to any would-be unauthorized user.

An invalid card will be retained by the terminal and retrieved by authorized personnel. If the finger prints don't match the card is retained, otherwise access is granted to the service offered by the terminal.

Figure 2 is a detailed flow chart depicting the above sequence of verification. In the preferred embodiment the card is an "intelligent card" with its own microprocessor or logic unit, memory, data and programs. In the preferred embodiment it is envisaged that the card will not carry its own power supply but will be connected to the terminal's power supply when the card is inserted. However, it may be preferable in some cases for the card to have its own power supply.

The whole process will start with the card's insertion into the terminal reader.

The verification process, then, shall start on the terminal side by generating a question directed to the card. On the card side, the checkout is accomplished by simply waiting for a certain period of time for the terminal's question. If the question does not arrive, the card will destroy all information in its memory and become useless.

If one assumes that the card and the terminal are the correct ones, the parallel processing of the input question must proceed on both the terminal and card sides. On the terminal side, the checking of the card is achieved similarly to the card's check by waiting for the answer for a certain period of time. If the answer does not arrive, the terminal can withhold the card or reject it. If the answer does arrive it will process it.

The invention can be configured to use different types of cards for different applications. For example:

- 1) Passport cards
- 2) Credit cards
- 3) Security access cards
- 4) Licence cards
- 5) Debit cards

Different types of cards would produce different answers to the initial question. This would be the way the terminal recognizes the type of card it is dealing with. If the answer from the card arrives

on time, the terminal would sort the answer to the proper application and proceed by checking if the answer is correct. In the negative case, it would, again, withhold or reject the card.

The next stage is the verification process in which identity of the card user is verified. This is done through a process of finger print checkout. The person's finger prints are scanned and compared with the template stored on the card. Again, if any attempt is made to read the data from the card memory before the finger print verification process is completed, the card will destroy its data.

The card will only allow access to its memory after confirmation from the terminal that the user is permitted to use it.

It is unlikely that the whole verification process will take any longer than approximately 25 seconds although the timing is not critical.

It is possible that someone could try to gain access to the data or the software itself by tampering with the terminal. To prevent this, all terminal software could be placed on RAM memory only. This way it would be lost immediately if the power to the terminal is disrupted. Only a licensed technician with his own access portable device would be able to download new software either from his portable device or from the host computer, and bring the terminal up again.

The block diagram of Figure 3 shows the hardware configuration of a preferred embodiment of a simple system comprised of only one terminal. The host computer system 1 is remotely located from the terminal 3. The two are connected by way of a telephone line 2 and modems 10a and 10b. The terminal 3 is composed of a PC-type motherboard 9, which includes a microprocessor or other logic device and memory, an "intelligent card" reader 6, a finger print scanner 7, a custom keyboard 8 and a display 5. The card reader 6 is adapted to receive and communicate with the "intelligent card" 4. The "intelligent card" typically contains a microprocessor or some other logic device and memory. Appropriate software and data are stored in the terminal 3 and in the "intelligent card" 4 to enable the verification procedures represented by the flow chart of Figure 2 to be carried out.

"Intelligent cards" are a unique technology utilizing plastic or some other media in which to embed microprocessor or some such logic unit and memory chips. The cards accordingly have both memory and processing capabilities. Essentially they are pocket sized computer systems with a wide range of application possibilities.

A number of off-the shelf items can be used in the system. The terminal could use an IBM PC[™] motherboard, a Toshiba[™] FZ1318 card reader and an IDENTIX Touchsave[™] T5-500 finger print scanner. The "intelligent card" could be a Toshiba

TOSMART[™] CZ-3000. Typically an IBM PC[™] could be used as the host computer but larger more complex systems using many terminals may require a larger computer such as a mainframe.

Interconnections other than tel phone lines and modems are possible. For example a security system for a building may have dedicated communication cables connecting the various terminals to the host computer without the use of modems. Also radio and optical interconnections are possible.

Finally to further enhance security an encryption technique could be used to encode data before transmitting between the host computer and the terminal, and decoding upon receipt. Similarly encoding and decoding could be used when reading and writing from and to the "intelligent card".

A number of changes and modifications apparent to one skilled in the art can be made without departing from the invention.

Claims

1. a system for the interchange of information comprising at least one portable electronic device; at least one terminal device; communication means to effect communications between the terminal device and the portable device; the portable device containing verification means to verify that the terminal device is a valid one; the terminal device containing verification means to verify that the portable device is a valid one and further verification means to verify that the user is authorized to use the system; protection means to prevent tampering with a terminal and encryption means to encode and decode data at the interface between the portable device and the terminal device.

2. The system of Claim 1 wherein the portable device contains a microprocessor or similar logic device, memory, data transfer means and interfaces to effect communications between the card and the terminal.

3. The system of claim 1 or Claim 2 wherein the terminal device contains input means, output means, a scanning device for scanning a physical characteristic of a user, a card reader, a microprocessor or other logic unit, memory and data transfer means.

4. The system of Claim 3 wherein the input means is a keyboard, the output means is a display.

5. The system of any one of Claims 1 to 4 wherein the communications means comprises a telephone line and one or more modems.

6. The system of any one of Claims 1 to 5 wherein the said verification means includes a computer program or programs.

7. The system of any of Claims 1 to 6 wherein

the said further verification means includes a finger print scanner and a computer program or programs to compare the information from the scan of the user's finger print with prestored finger print information in the portable electronic device.

8. The system of any one of Claims 1 to 7 wherein the protection means includes volatile memory which loses its contents when the power is interrupted.

9. The system of any one of Claims 1 to 8 wherein the terminal is connected to a host computer by further communication means and further encryption means.

10. The system of Claim 9 wherein the further communication means includes one or more of telephone lines and modems, direct cable, and radio and optical transmissions, and the further encryption means is used to encode and decode information at the interface between the terminal and the host computer.

11. A secure system for the interchange of information comprising a plurality of portable devices, a plurality of terminal devices, a communication link connecting the said terminal devices with a host computer; such portable electronic device comprised of a memory for the storage of data, a microprocessor or similar logic unit for the manipulation of data and data transfer means; the said memory containing data which identifies the user and a program by which the portable device can verify that the terminal device is a valid one and to effect interchanges of information or if the terminal is invalid to erase the memory; the terminal devices each comprising a microprocessor or similar logic unit, a memory for the storage of data, a program to verify that the card is a valid one, a scanning device input and output devices to communicate with the user, a power source and being adapted to connect to the portable device so as to supply power to the portable device when necessary and to transfer data between the said portable device and the said terminal device.

12. The system of Claim 11 wherein the portable device contains its own power supply.

13. A method of providing for secure interchange of information in a portable device - terminal environment comprising the steps of: the terminal verifying that the portable device is valid; the portable device verifying that the terminal is valid; the terminal obtaining data by a physical characteristic scan of the user and comparing this data to data stored on the user's portable device; using encryption means to encode and decode information at interfaces where unauthorized access could be gained; the portable device erasing its program and data if an invalid terminal attempts to communicate with it; the terminal keeping or rejecting portable devices determined to be invalid or if valid

the user is unauthorized; the terminal data and program being lost when power is interrupted; and the terminal being brought back up after power loss only by an authorized person utilizing an access portable device.

5

10

15

20

25

30

35

40

45

50

55

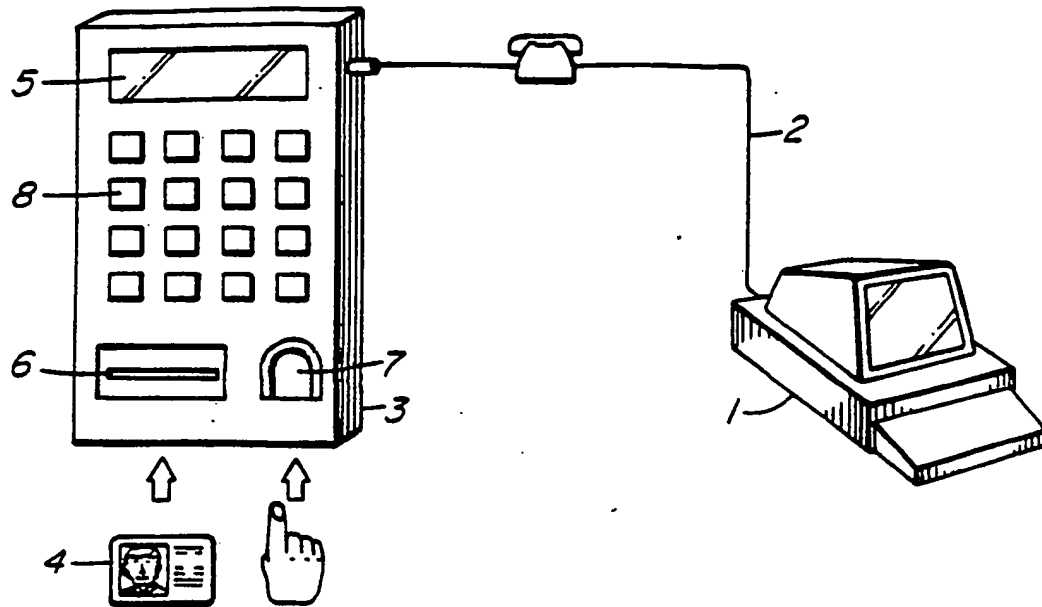


FIG. 1

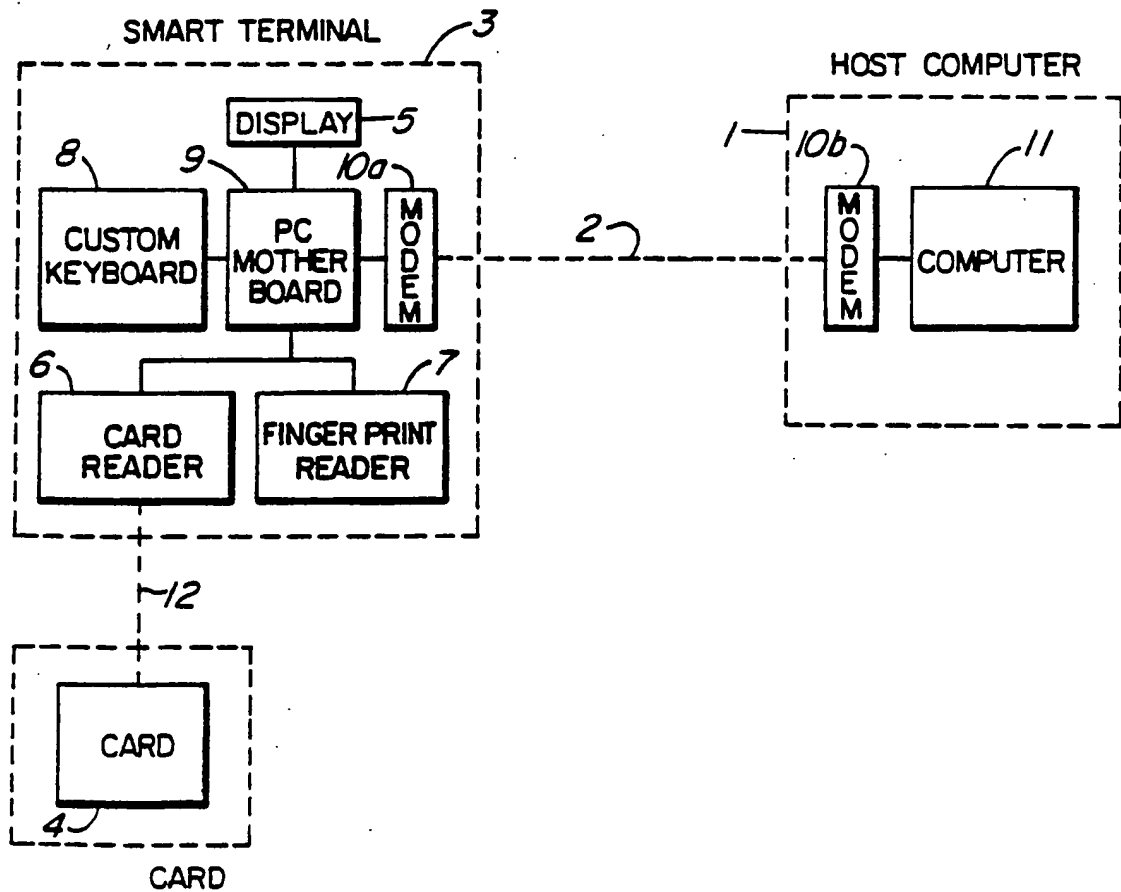


FIG. 3

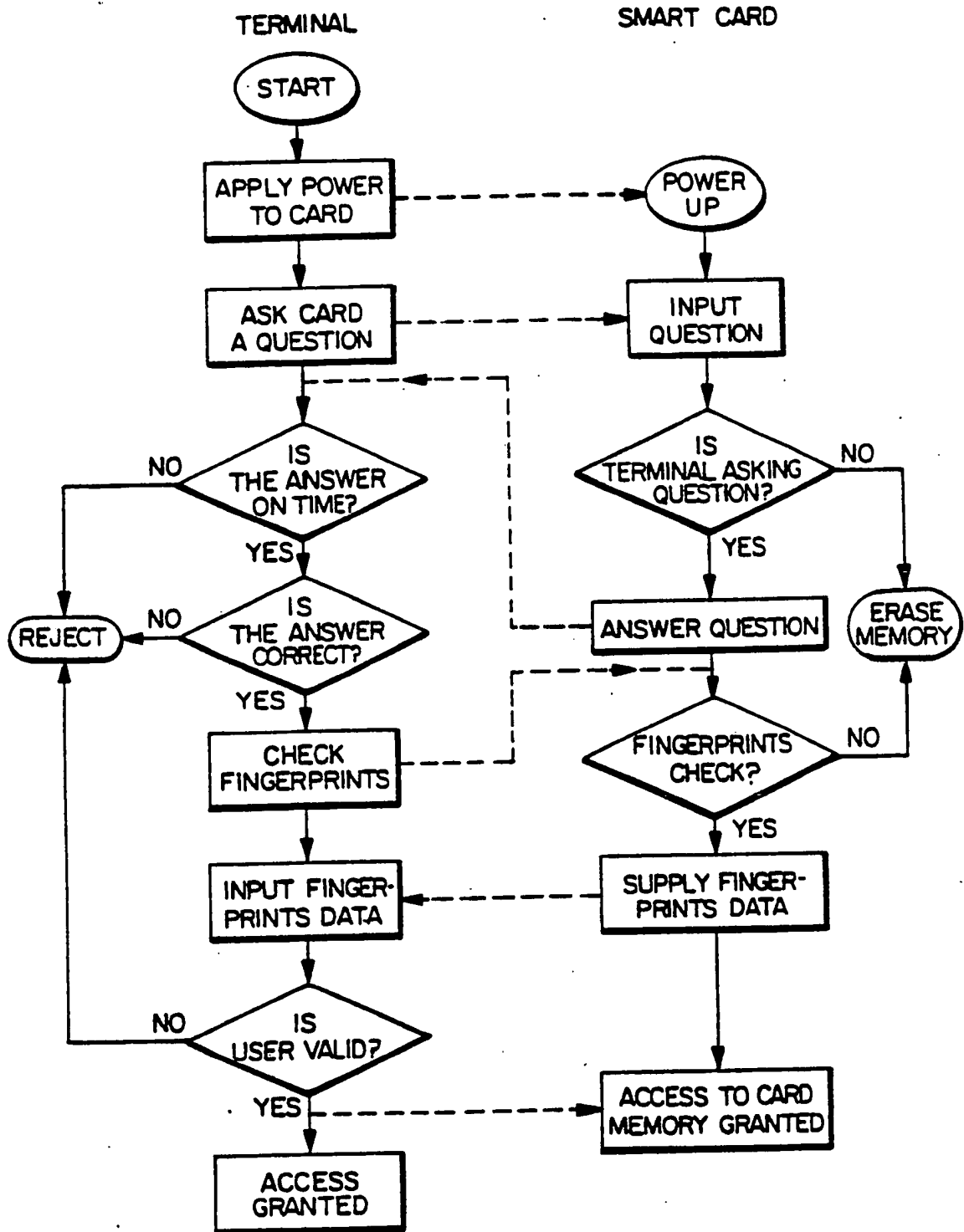


FIG. 2



DOCUMENTS CONSIDERED TO BE RELEVANT			EP 90300442.2
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl. 7)
A	GB - A - 2 181 582 (VICTOR CAMPBELL BLACKWELL) * Totality * --	1, 2, 3, 4, 7, 9, 11, 13	G 07 F 7/10 G 07 F 7/08
A	US - A - 4 138 058 (ATALLA) * Totality * --	1, 3, 4, 7, 11, 13	
A	EP - A2 - 0 223 122 (INTERNATIONAL BUSINESS MACHINES CORPORATION) * Totality * --	1, 2, 4, 11, 13	
A	EP - A2 - 0 216 298 (CASIO COMPUTER COMPANY LIMITED) * Totality * --	1, 2, 3, 4, 11, 13	
A	EP - A2 - 0 243 873 (CASIO COMPUTER COMPANY LIMITED) * Totality * --	1, 11, 13	
A	EP - A2 - 0 220 703 (CASIO COMPUTER COMPANY LIMITED) * Totality * --	1, 2, 11, 12, 13	G 07 F 7/00
D, A	CA - A - 1 207 460 (CII HONEYWELL BULL) * Totality * --	1, 2, 3, 11, 13	
D, A	GB - A - 2 185 937 (MICHAEL ANTHONY O'SHEA et al.) * Totality * --	1, 7	
D, A	GB - A - 1 504 196 (SOCIETE INTERNATIONALE POUR L'AVIATION)	1, 11, 13	
The present search report has been drawn up for all claims			
Place of search VIENNA		Date of completion of the search 23-03-1990	Examiner BEHMER
CATEGORY OF CITED DOCUMENTS		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document			



-2-

EP 90300442.2

DOCUMENTS CONSIDERED TO BE RELEVANT			CLASSIFICATION OF THE APPLICATION (Int Cl')
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	
D,A	* Totality * -- <u>GB - A - 1 505 715</u> (SOCIETE INTERNATIONALE POUR L'AVIATION)	1, 11, 13	
D,A	* Totality * -- <u>US - A - 3 702 464</u> (CASTRUCCI)	1, 2, 11	
	* Totality * -----		
The present search report has been drawn up for all claims			TECHNICAL FIELDS SEARCHED (Int Cl')
Place of search VIENNA		Date of completion of the search 23-03-1990	Examiner BEHMER
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	